

#### ZIT-BB Dezernat 2.3



13.12.2022

Version 1.0

# Multi-Faktor-Authentifizierung Anleitung für Benutzer

### **Einleitung**

Der Zugang zu Online-Portalen und Anwendungen mit Benutzername und Kennwort bietet eine heute nicht mehr ausreichende Sicherheit für den Schutz sensibler Daten. Die Mehr-Faktor-Authentifizierung (MFA), auch Multi-Faktor-Authentifizierung oder Zwei-Faktor-Authentifizierung (2FA) genannt, bietet eine höhere Sicherheit. Es gibt viele Varianten z.B. den Personalausweis, den Fingerabdruck, den Irisscann oder eine Zugangskarte.

In unseren Portalen benutzen wir als ersten Faktor die Benutzerkennung (E-Mail) und ein Kennwort. Der zweite Faktor ist ein Einmalkennwort. Der Benutzer bekommt das Einmalkennwort per E-Mail.

Alternativ kann der Benutzer den zweiten Faktor, das Einmalkennwort, über einen Authenticator bekommen. Der Authenticator ist eine App auf dem Smartphone, Laptop oder PC und erzeugt ein zeitbasiertes Einmalkennwort (Timebased OTP). Siehe <u>Einrichten eines Authenticators</u>.

Diese Anleitung beschreibt den Vorgang der Anmeldung und das Einrichten eines Authenticator.

**Hinweis:** Auch nach dem Einrichten eines Authenticator kann der Benutzer bei jeder Anmeldung zwischen dem Einmalkennwort per Mail und dem zeitbasiertes Einmalkennwort aus dem Authenticator wählen.

# Ablauf der Anmeldung

- 1. Die erste Loginmaske enthält Benutzerkennung(E-Mail-Adresse) und Kennwort.
- 2. Die zweite Loginmaske enthält eine Schaltfläche zu Anfordern der E-Mail mit dem Einmalkennwort und ein Feld zur Eingabe des Einmalkennwortes.

E-Mail-Adresse	
Kennwort	
Anmelden	

Abbildung 1: Faktor 1 - E-Mail und Kennwort

Bitte klicken Sie auf "Einmalennwort anfordern". Ein Einmalkennwort wird an Ihre E-Mail-Adresse juer*******chke@zit-bb.brandenburg.de gesendet.
Einmalkennwort anfordern
Geben Sie das Einmalkennwort aus der E-Mail ein.
Einmalkennwort senden

Abbildung 2: Faktor 2 - Einmalkennwort

O:\ZIT-BB\GB2\D2\_3\Ablage\01 Akten\252 Basiskomponenten\252 12aPortalservice DXP\03-IT-Betriebshandbuch\Multi-Faktor-Authentifizerung\Anleitung MFA fuer Benutzer.docx Alternativ kann nach dem Konfigurieren eines Authenticators ein zeitbasiertes Einmalkennwort verwendet werden. Siehe <u>Einrichten eines Authenticators</u>.



Abbildung 3: Faktor 2 - mit Einmalkennwort aus dem Authenticator

## Zeitbasiertes Einmalkennwort - Einführung

Für das zeitbasiertes Einmalkennwort (TOTP) wird eine Token Generator benötigt. Der Token Generator, auch Authenticator genannt, ist eine Software die den standardisierten Algorithmus <u>RFC</u> 6238 implementiert und über eine synchronisierte Uhr das Einmalkennwort erzeugt. Der Benutzer installiert die Software auf seinem PC, Laptop oder Smartphone, ruft den Dialog zur Synchronisation im Portal auf und kann dann wahlweise das Einmalkennwort per Mail oder das zeitbasiertes Einmalkennwort des Authenticators für die Authentifizierung benutzen.

Es sind eine Reihe verschiedener Anwendungen und Mobile-Apps verfügbar, die diesen Algorithmus implementieren. Neben den namhaften Apps von Google und Microsoft, gibt es auch einige quelloffene Apps (Open Source). Eine gute Übersicht liefert der deutsche Wikipedia-Artikel Zwei-Faktor-Authentisierung

### **Einrichten eines Authenticators**

Als Authenticator können Sie jede Anwendung/App verwenden, die den Standard <u>RFC 6238</u> implementiert. Als Beispiel benutzen wir den Authenticator von Microsoft.

### 1. Installation auf dem Smartphone

Öffnen Sie den Play Store und suchen Sie nach "Authenticator App" Wählen Sie Microsoft Authenticator, oder eine andere App.

### 2. Vorbereitung im Portal

Klicken Sie auf das Symbol "Benutzermenü" Wählen Sie "Kontoeinstellungen" und dann "Mehrstufige Authentifizierung" Scannen Sie den QR-Code oder geben Sie das "Shared Secret" ein.

### 3. Verbindung herstellen

Öffnen Sie den Authenticator auf dem Smartphone Wählen Sie + Konto hinzufügen (Persönliches Konto) Wählen Sie QR-Code scannen und scannen Sie den Code vom Portal. Rufen Sie das neue Konto auf und geben Sie das Einmalkennwort aus der App im Portal ein. Klicken Sie auf Senden. Schließen Sie das Fenster mit "X".



Kontoeinstellungen				
Allgemein	Mehrstufige Authentifizierung			
Zeitbas	iertes Einmalkennwort			
Anleitung   1. Installieren Sie einen Authenticator auf Ihrem Smarphone, Tablet oder PC.   z.B. den Authenticator App von Google oder Microsoft.   2. Offnen Sie den Authenticator und fügen Sie ein Konto hinzu.   Sie müssen dabei den QR-Code scannen oder das "Shared Secret" von dieser Seite eingeben.   3. Tragen Sie das Einmalkennword us dem Authenticator hier ein und Klicken Sie auf "Senden".   Nun können Sie bei jeder Anmeldung die Methoden zur Authentifizierung auswählen.				
Zeitbasierte	es Einmalkennwort			
Shared Se	2. Einmalkennwort eingeben			
UTAW3G	RFT64KCOJG2MACU4XSJHUX4YWP			
1. Scannen 3. Speichern				
		Senden		

Abbildung 4: Verbinden

Kontoeinstellungen		×	
Allgemein	Mehrstufige Authentifizierung		
Zeitbasiertes Einmalkennwort			
Sie können für Ihr Konto nur ein zeitbasiertes Einmalkennwort konfigurieren. Entfernen Sie Ihr existierendes zeitbasiertes Einmalkennwort, um ein neues zeitbasiertes Einmalkennwort zu generieren.			
		Konfiguriertes zeitbasiertes Einmalkennwort entfernen	

Abbildung 5: Fenster schließen